AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for facilitating a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, comprising:

initially establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

encrypting an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

sending the encrypted identifier from the first party across the network to the second party;

allowing the second party to decrypt the encrypted identifier by using the group secret key and the negotiated secret key;

allowing the second party to use the identifier to ~~lookup~~ look up the pre-shared secret key that was previously established between the first party and the second party; and

using the pre-shared secret key in forming at least one subsequent communication between the first party and the second party.

2. (Cancelled).

3. (Currently amended) The method of ~~claim 2~~ claim 1, wherein establishing the negotiated secret key involves using the Diffie-Hellman method to establish the negotiated secret key.

4. (Original) The method of claim 1, wherein the second party is a firewall through which the first party seeks to communicate.

5. (Original) The method of claim 4, wherein the first party is a person seeking to communicate through the firewall from one of a number of possible Internet Protocol (IP) addresses.

a3

6. (Original) The method of claim 1, wherein the group secret key is one of a plurality of group secret keys maintained by the group.

7. (Currently amended) A method for facilitating a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, comprising:

initially establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

allowing the first party to encrypt an identifier for the first using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

receiving the encrypted identifier at the second party from the first party across the network;

decrypting the encrypted identifier by using the group secret key and the negotiated secret key;

using the identifier to lookup the pre-shared secret key that was previously established between the first party and the second party; and

using the pre-shared secret key in forming at least one subsequent communication between the first party and the second party.

8. (Cancelled)

9. (Currently amended) The method of ~~claim 8~~ claim 7, wherein establishing the negotiated secret key involves using the Diffie-Hellman method to establish the negotiated secret key.

10. (Original) The method of claim 7, wherein the second party is a firewall through which the first party seeks to communicate.

11. (Original) The method of claim 10, wherein the first party is a person seeking to communicate through the firewall from one of a number of possible Internet Protocol (IP) addresses.

12. (Original) The method of claim 7, wherein the group secret key is one of a plurality of group secret keys maintained by the group.

13. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, the method comprising:

initially establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

encrypting an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

sending the encrypted identifier from the first party across the network to the second party;

allowing the second party to decrypt the encrypted identifier by using the group secret key and the negotiated secret key;

allowing the second party to use the identifier to ~~lookup~~ look up the pre-shared secret key that was previously established between the first party and the second party; and

using the pre-shared secret key in forming at least one subsequent communication between the first party and the second party.

14. (Cancelled).

15. (Currently amended) The computer-readable storage medium of ~~claim 14~~ claim 13, wherein establishing the negotiated secret key involves using the Diffie-Hellman method to establish the negotiated secret key.

16. (Original) The computer-readable storage medium of claim 13, wherein the second party is a firewall through which the first party seeks to communicate.

17. (Original) The computer-readable storage medium of claim 16, wherein the first party is a person seeking to communicate through the firewall from one of a number of possible Internet Protocol (IP) addresses.

a3

18. (Original) The computer-readable storage medium of claim 13, wherein the group secret key is one of a plurality of group secret keys maintained by the group.

19. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, the method comprising:

establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

allowing the first party to encrypt an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

receiving the encrypted identifier at the second party from the first party across the network;

decrypting the encrypted identifier by using the group secret key and the negotiated secret key;

using the identifier to lookup the pre-shared secret key that was previously established between the first party and the second party; and

using the pre-shared secret key in forming at least one subsequent communication between the first party and the second party.

20. (Currently amended) An apparatus that facilitates a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, the apparatus comprising:

establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

an encryption mechanism that is configured to encrypt an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

a communication mechanism that is configured to send the encrypted identifier from the first party across the network to the second party, so that the second party can decrypt the encrypted identifier by using the group secret key and the negotiated secret key in order to use the identifier to lookup the pre-shared secret key that was previously established between the first party and the second party; and

wherein the communication mechanism is additionally configured to use the pre-shared secret key to encrypt at least one subsequent communication between the first party and the second party.

a3

21. (Cancelled)

22. (Currently amended) The apparatus of ~~claim 21~~ claim 20, wherein establishing the negotiated secret key involves using the Diffie-Hellman method to establish the negotiated secret key.

23. (Original) The apparatus of claim 20, wherein the second party is a firewall through which the first party seeks to communicate.

24. (Original) The apparatus of claim 23, wherein the first party is a person seeking to communicate through the firewall from one of a number of possible Internet Protocol (IP) addresses.

25. (Original) The apparatus of claim 20, wherein the group secret key is one of a plurality of group secret keys maintained by the group.

26. (Currently amended) An apparatus that facilitates a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, the apparatus comprising:

establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network;

wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key;

a communication mechanism that is configured to receive an encrypted identifier at the second party from the first party across the network;

wherein the encrypted identifier was produced by encrypting an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key;

wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group;

a decryption mechanism that is configured to decrypt the encrypted identifier by using the group secret key and the negotiated secret key;

a lookup mechanism that is configured to use the identifier to ~~lookup~~ look up the pre-shared secret key that was previously established between the first party and the second party; and

wherein the communication mechanism is additionally configured to use the pre-shared secret key in forming at least one subsequent communication between the first party and the second party.